## Chapter 1

# Operations and Electronic Warfare

Division targeting teams and electronic warfare (EW) personnel work together to ensure that EW is integrated into targeting, is thoroughly planned, and is vigorously executed. The use of standard EW targets without thorough analysis and planning significantly limits the potential of EW as a true combat multiplier. Inadequate planning leads to the uncoordinated use of EW and limits the effects of both EW and fire support (FS) as a whole. On the other hand, if EW is adequately staffed, trained, integrated into targeting, planned, and executed, it helps the commander reach his targeting objectives by dominating the electromagnetic environment (EME).

EW can attack the threat when it is most vulnerable through a quick, accurate, timely, and responsive means that can also provide a fast assessment of the operation. Additionally, EW is important because it is a responsive tool to perform suppression of enemy air defenses (SEAD); it is also one of the integrated tools used to conduct information operations (IO). However, EW is effective only when the commander decides there is more value in conducting EA (for a specific high-payoff target [HPT] at a specific point) than performing additional collection in order to produce more intelligence.

## THE POTENTIAL

1-1. The potential for EA is unlimited especially within the information age.

- **Offensive** operations often provide the friendly forces the element of surprise. Prior to units crossing the line of departure (LD), EA assets begin their missions. EA may focus on the scout or reconnaissance net to ensure intelligence indicating friendly forces attacking is not passed to the threat command post (CP). As units begin to engage the threat, EA assets then shift their effort onto the threat's counterbattery, command and control ($C^2$), and artillery. The suppression of these targets denies the enemy the ability to effectively control his forces and also disrupts the flow of information to his artillery and counterbattery, thus rendering them useless. At this point, EA systems engage specific targets. A unit near a bridge that was destroyed is jammed to prevent the requesting of engineer support. This will cause a delay in maneuvering an enemy unit that would protect a vulnerable flank.

- **Defensive** operations, conducted with the immediate purpose of causing an enemy attack to fail, often allow the friendly force to close off areas and create devastating engagement areas while denying the threat critical information. EA assets cover constricted terrain areas along the threat avenue of approach (AA). The engineers erect obstacles in order for maneuver and artillery units to create an engagement area. EA assets begin their mission as soon as the threat enters the area and no longer has direct contact with other units. At this time units engage with artillery and destroy threat forces. Because the threat has no communications, the engagement will be swift, with high casualties and lost momentum, thus ending the threat attack. EA also will be used in counterreconnaissance to deny threat scouts the ability to pass vital intelligence back to their commander.

## METHODOLOGY

1-2. There is not a separate methodology to conduct EW. The best way to conduct EW is to effectively integrate EW within the targeting methodology and TTP. This manual and the flow of products are in accordance with FM 6-20-10. They provide a clear and relatively simple framework, terminology, and TTP to plan and conduct EA as a subset of EW. The framework begins with the targeting functions of DECIDE, DETECT, DELIVER, and ASSESS.

## THE ENVIRONMENT

1-3. Operations are executed in an increasingly complex EME. Almost all military units use electromagnetic (EM) devices for communications, navigation, sensing, information storage, and processing. The increasing mobility and affordability of sophisticated EM equipment guarantees that the environment will become even more complex in the future. This environment creates vulnerabilities to and opportunities for EW for both friendly and threat forces. The threat and the friendly commanders depend on this flow of information to make informed decisions. EW can exploit this dependence. Appendix A further describes this environment.

1-4. The need to control the EM spectrum and the type of EW actions that can be used to control that spectrum depend on the operational environment. During peacetime, government bodies and international treaties and conventions control the use of the EM spectrum. However, standing rules of engagement (ROE) give joint commanders the authority in peacetime to take appropriate and necessary action to protect their forces. The type and level of EW actions appropriate to a particular operation depend on threat capabilities, threat vulnerabilities, and operational objectives.

## ELECTRONIC WARFARE

1-5. EW includes three major subdivisions: electronic protection (EP), electronic warfare support (ES), and electronic attack (EA). EW is waged (through the use of EM or directed energy) within the EM spectrum to—

- Secure and maintain effective control and use of the spectrum for friendly forces.
- Attack the threat and to deny the use of the spectrum through damage, destruction, disruption, and deception.

## ELECTRONIC PROTECTION

1-6. EP involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability. This manual contains very little discussion of this subdivision of EW.

## ELECTRONIC WARFARE SUPPORT

1-7. ES involves the search for, intercepts, identification, and location of sources of radiated EM energy (intentional and unintentional) in order to recognize and collect information on the threat. ES provides information necessary for immediate decisions involving EW operations and other tactical actions. Both EA and ES are critical and mutually supportive components.

## ELECTRONIC ATTACK

1-8. EA involves the use of EM, directed energy (DE), or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered to be a form of fires. EA includes—

- Taking actions to prevent or reduce an enemy's effective use of the EM spectrum (for example, jamming and EM deception).
- Employing weapons that use either EM or DE to destroy EM equipment (for example, lasers, radio frequency [RF] weapons, or particle beams).

### First Recorded Instance of Deliberate Radio Jamming

The first recorded instance of deliberate radio jamming took place in September 1901 in the US. Interestingly, it was aimed at securing commercial gain rather than military advantage. As now, there was considerable public interest in the America's Cup yacht races, and the newspaper first to reach the stands carrying each result stood to reap a large profit.... A third company...failed to get a sponsor but...used a transmitter more powerful than its competitors, and one of its engineers, John Pickard, worked out a method which allowed him to jam signals from the other companies while at the same time to report on the progress of the race from his boat.

Source: The History of US Electronic Warfare, Volume I

## TACTICAL ELECTRONIC ATTACK

1-9. EA is best used as a combat multiplier in conjunction with other fires into an engagement area. Used alone, EA is only a delaying or disrupting fire—its effects are reduced. Additionally, the technique of using EA fires independently of other fires provides the enemy time and training to overcome the effects of future EA. While EA operations within a theater or joint task force area of operation (AO) are often complicated, tactical EA operations (to include division operations) are relatively simple.

1-10. The scope of tactical EA operations are limited by doctrine, organic and supporting capabilities, and realistic unit standing operating procedures (SOPs). However, when a tactical echelon lacks adequate organic or supporting capabilities, it can request support from a higher echelon. Sometimes a tactical echelon might not even know of an existing capability at a higher echelon. The US Air Force (USAF), US Marine Corps (USMC), and US Navy (USN) have the EA equipment for the SEAD. With the Army's dependence on aviation assets, the request for support from echelons above corps (EAC) in the joint arena for SEAD support will remain constant.

## CURRENT AND FUTURE THREAT ELECTRONIC WARFARE CAPABILITIES

1-11. While allied forces are able to conduct EA, many threats, using off-the-shelf equipment, have the ability to conduct EA with greater distance and against targets conventionally safe against EA. The current communications environment provides many potential threats with a rich environment to conduct EW and exploit friendly communications. The more a unit relies on communications, the more vulnerable that unit is to threat ES and EA. In general, many threats currently have the capability to—

- Detect and locate friendly units because of our use of EM equipment.
- Monitor and exploit friendly unit's communications to include collecting information on a unit's mission, combat strength, logistics, morale, weakness, and other critical information.
- Deny a friendly unit's use of the EM spectrum, thereby degrading that unit's ability to plan operations, execute $C^2$, receive and process intelligence, and execute operations.

1-12. The future communications environment will provide threats with a target-rich environment for EW. In general, future threats will be able to—

- Detect, locate, and jam low probability of intercept (LPI) signals. The Army currently uses many types of LPIs (for example, Single-Channel Ground and Airborne Radio System [SINCGARS]).
- Use DE to destroy computer networks by using electromagnetic pulses (EMPs) to destroy silicon chips inside equipment.
- Use electronic deception to enter and control friendly voice and data nets.